

CLAIMS

What is claimed is:

- 5 1. A method for authenticating a client within a distributed data processing system, the method comprising the steps of:
- receiving a digital certificate from the client at a host within the distributed data processing system;
- 10 obtaining a host identity for the client from the digital certificate;
- retrieving host-encrypted secret data associated with the host identity from the digital certificate;
- decrypting the host-encrypted secret data with a host private key; and
- 15 authenticating the client using the host identity and the decrypted secret data.
2. The method of claim 1, wherein the host acts as a proxy for the client.
3. The method of claim 1 further comprising:
- verifying the received digital certificate.
4. The method of claim 1 further comprising:
- generating, at the client, a request for a digital certificate comprising host identity mapping data;
- 20 sending the request for the digital certificate to a certifying authority (CA); and
- receiving a digital certificate comprising host identity mapping data from the certifying authority.
5. The method of claim 4 further comprising:

AUS9-2000-0255-US1

storing the host identity in the request for the digital certificate;

encrypting secret data associated with the host identity using a public key of the certifying authority to generate CA-encrypted secret data; and

storing the CA-encrypted secret data in the request for the digital certificate, wherein the host identity and the CA-encrypted secret data comprise the host identity mapping data in the request for the digital certificate.

6. The method of claim 4 further comprising:

receiving, at the certifying authority, the request for a digital certificate;

generating the digital certificate in response to the received request for the digital certificate; and

sending the generated digital certificate to the client.

7. The method of claim 4 further comprising:

retrieving CA-encrypted secret data from the host identity mapping data in the request for the digital certificate;

decrypting the CA-encrypted secret data associated with the host identity using a private key of the certifying authority to generate decrypted secret data;

encrypting the decrypted secret data associated with the host identity using a public key of the host to generate the host-encrypted secret data; and

storing the host-encrypted secret data in the digital certificate, wherein the host identity and the host-encrypted secret data comprise the host identity mapping data in the digital certificate.

AUS9-2000-0255-US1

8. The method of claim 1 wherein the digital certificate comprises multiple host identities for multiple hosts within the distributed data processing system.

5 9. The method of claim 1 wherein the digital certificate is formatted according to the X.509 standard.

10 10. The method of claim 9 wherein the host identity and the host-encrypted secret data associated with the host identity is stored within an X.509 extension within the digital certificate.

11. The method of claim 1 further comprising:
performing multiple authentication processes within the distributed data processing system for the client through the host using information within the digital certificate.

12. A method for generating a digital certificate, the method comprising the steps of:

20 receiving, at a certifying authority (CA), a request for a digital certificate from a client, wherein the request for a digital certificate comprises host identity mapping data;

25 generating the digital certificate in response to the received request for a digital certificate; and

sending the generated digital certificate to the client, wherein the digital certificate comprises host identity mapping data from the certifying authority.

30 13. The method of claim 12 further comprising:

retrieving CA-encrypted secret data from the host identity mapping data in the request for a digital certificate;

AUS9-2000-0255-US1

decrypting the CA-encrypted secret data associated with a host identity using a private key of the certifying authority to generate decrypted secret data;

5 encrypting the decrypted secret data associated with the host identity using a public key of a host to generate a host-encrypted secret data; and

10 storing the host-encrypted secret data in the digital certificate, wherein the host identity and the host-encrypted secret data comprise the host identity mapping data in the digital certificate.

14. An apparatus for authenticating a client within a distributed data processing system, the apparatus comprising:

15 first receiving means for receiving a digital certificate from the client at a host within the distributed data processing system;

obtaining means for obtaining a host identity for the client from the digital certificate;

20 first retrieving means for retrieving host-encrypted secret data associated with the host identity from the digital certificate;

first decrypting means for decrypting the host-encrypted secret data with a host private key; and

25 authenticating means for authenticating the client using the host identity and the decrypted secret data.

15. The apparatus of claim 14, wherein the host acts as a proxy for the client.

30

16. The apparatus of claim 14 further comprising:

verifying means for verifying the received digital certificate.

AUS9-2000-0255-US1

17. The apparatus of claim 14 further comprising:

first generating means for generating, at the client, a request for a digital certificate comprising host identity mapping data;

first sending means for sending the request for the digital certificate to a certifying authority (CA); and

second receiving means for receiving a digital certificate comprising host identity mapping data from the certifying authority.

18. The apparatus of claim 17 further comprising:

first storing means for storing the host identity in the request for the digital certificate;

first encrypting means for encrypting secret data associated with the host identity using a public key of the certifying authority to generate CA-encrypted secret data; and

second storing means for storing the CA-encrypted secret data in the request for the digital certificate, wherein the host identity and the CA-encrypted secret data comprise the host identity mapping data in the request for the digital certificate.

19. The apparatus of claim 17 further comprising:

third receiving means for receiving, at the certifying authority, the request for a digital certificate;

second generating means for generating the digital certificate in response to the received request for the digital certificate; and

second sending means for sending the generated digital certificate to the client.

AUS9-2000-0255-US1

20. The apparatus of claim 17 further comprising:

second retrieving means for retrieving CA-encrypted secret data from the host identity mapping data in the request for the digital certificate;

5 second decrypting means for decrypting the CA-encrypted secret data associated with the host identity using a private key of the certifying authority to generate decrypted secret data;

10 second encrypting means for encrypting the decrypted secret data associated with the host identity using a public key of the host to generate the host-encrypted secret data; and

15 third storing means for storing the host-encrypted secret data in the digital certificate, wherein the host identity and the host-encrypted secret data comprise the host identity mapping data in the digital certificate.

20 21. The apparatus of claim 14 wherein the digital certificate comprises multiple host identities for multiple hosts within the distributed data processing system.

22. The apparatus of claim 14 wherein the digital certificate is formatted according to the X.509 standard.

25 23. The apparatus of claim 22 wherein the host identity and the host-encrypted secret data associated with the host identity is stored within an X.509 extension within the digital certificate.

30 24. The apparatus of claim 14 further comprising:
performing means for performing multiple authentication processes within the distributed data processing system for

the client through the host using information within the digital certificate.

25. An apparatus for generating a digital certificate, the
5 apparatus comprising:

receiving means for receiving, at a certifying authority (CA), a request for a digital certificate from a client, wherein the request for a digital certificate comprises host identity mapping data;

10 generating means for generating the digital certificate
in response to the received request for a digital
certificate; and

sending means for sending the generated digital certificate to the client, wherein the digital certificate comprises host identity mapping data from the certifying authority.

26. The apparatus of claim 25 further comprising:

```

    retrieving means for retrieving CA-encrypted secret
20  data from the host identity mapping data in the request for
    a digital certificate:

```

decrypting means for decrypting the CA-encrypted secret data associated with a host identity using a private key of the certifying authority to generate decrypted secret data;

25 encrypting means for encrypting the decrypted secret
data associated with the host identity using a public key of
a host to generate a host-encrypted secret data; and

storing means for storing the host-encrypted secret data in the digital certificate, wherein the host identity and the host-encrypted secret data comprise the host identity mapping data in the digital certificate.

[illegible]

5

10

15

20

25

30

instructions for sending the request for the digital certificate to a certifying authority (CA); and

AUS9-2000-0255-US1

instructions for receiving a digital certificate comprising host identity mapping data from the certifying authority.

5 31. The computer program product of claim 30 further comprising:

instructions for storing the host identity in the request for the digital certificate;

10 instructions for encrypting secret data associated with the host identity using a public key of the certifying authority to generate CA-encrypted secret data; and

15 instructions for storing the CA-encrypted secret data in the request for the digital certificate, wherein the host identity and the CA-encrypted secret data comprise the host identity mapping data in the request for the digital certificate.

32. The computer program product of claim 30 further comprising:

20 instructions for receiving, at the certifying authority, the request for a digital certificate;

instructions for generating the digital certificate in response to the received request for the digital certificate; and

25 instructions for sending the generated digital certificate to the client.

33. The computer program product of claim 30 further comprising:

30 instructions for retrieving CA-encrypted secret data from the host identity mapping data in the request for the digital certificate;

AUS9-2000-0255-US1

instructions for decrypting the CA-encrypted secret data associated with the host identity using a private key of the certifying authority to generate decrypted secret data;

5 instructions for encrypting the decrypted secret data associated with the host identity using a public key of the host to generate the host-encrypted secret data; and

10 instructions for storing the host-encrypted secret data in the digital certificate, wherein the host identity and the host-encrypted secret data comprise the host identity mapping data in the digital certificate.

34. The computer program product of claim 27 wherein the digital certificate comprises multiple host identities for multiple hosts within the distributed data processing system.

35. The computer program product of claim 27 wherein the digital certificate is formatted according to the X.509 standard.

36. The computer program product of claim 35 wherein the host identity and the host-encrypted secret data associated with the host identity is stored within an X.509 extension within the digital certificate.

37. The computer program product of claim 27 further comprising:

30 instructions for performing multiple authentication processes within the distributed data processing system for the client through the host using information within the digital certificate.

AUS9-2000-0255-US1

38. A computer program product on a computer readable medium for use in a distributed data processing system for generating a digital certificate, the computer program product comprising:

5 instructions for receiving, at a certifying authority (CA), a request for a digital certificate from a client, wherein the request for a digital certificate comprises host identity mapping data;

10 instructions for generating the digital certificate in response to the received request for a digital certificate; and

15 instructions for sending the generated digital certificate to the client, wherein the digital certificate comprises host identity mapping data from the certifying authority.

39. The computer program product of claim 38 further comprising:

20 instructions for retrieving CA-encrypted secret data from the host identity mapping data in the request for a digital certificate;

instructions for decrypting the CA-encrypted secret data associated with a host identity using a private key of the certifying authority to generate decrypted secret data;

25 instructions for encrypting the decrypted secret data associated with the host identity using a public key of a host to generate a host-encrypted secret data; and

30 instructions for storing the host-encrypted secret data in the digital certificate, wherein the host identity and the host-encrypted secret data comprise the host identity mapping data in the digital certificate.

40. A data structure representing a digital certificate for use in a data processing system, the data structure comprising:

- an issuer name;
5 a signature;
 a subject name; and
 an extension, wherein the extension comprises a host
identity and host-encrypted secret data associated with the
host identity.

10

1971	1972	1973	1974	1975	1976	1977	1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	2037	2038	2039	2040	2041	2042	2043	2044	2045	2046	2047	2048	2049	2050	2051	2052	2053	2054	2055	2056	2057	2058	2059	2060	2061	2062	2063	2064	2065	2066	2067	2068	2069	2070	2071	2072	2073	2074	2075	2076	2077	2078	2079	2080	2081	2082	2083	2084	2085	2086	2087	2088	2089	2090	2091	2092	2093	2094	2095	2096	2097	2098	2099	2100	2101	2102	2103	2104	2105	2106	2107	2108	2109	2110	2111	2112	2113	2114	2115	2116	2117	2118	2119	2120	2121	2122	2123	2124	2125	2126	2127	2128	2129	2130	2131	2132	2133	2134	2135	2136	2137	2138	2139	2140	2141	2142	2143	2144	2145	2146	2147	2148	2149	2150	2151	2152	2153	2154	2155	2156	2157	2158	2159	2160	2161	2162	2163	2164	2165	2166	2167	2168	2169	2170	2171	2172	2173	2174	2175	2176	2177	2178	2179	2180	2181	2182	2183	2184	2185	2186	2187	2188	2189	2190	2191	2192	2193	2194	2195	2196	2197	2198	2199	2200	2201	2202	2203	2204	2205	2206	2207	2208	2209	2210	2211	2212	2213	2214	2215	2216	2217	2218	2219	2220	2221	2222	2223	2224	2225	2226	2227	2228	2229	2230	2231	2232	2233	2234	2235	2236	2237	2238	2239	2240	2241	2242	2243	2244	2245	2246	2247	2248	2249	2250	2251	2252	2253	2254	2255	2256	2257	2258	2259	2260	2261	2262	2263	2264	2265	2266	2267	2268	2269	2270	2271	2272	2273	2274	2275	2276	2277	2278	2279	2280	2281	2282	2283	2284	2285	2286	2287	2288	2289	2290	2291	2292	2293	2294	2295	2296	2297	2298	2299	2300	2301	2302	2303	2304	2305	2306	2307	2308	2309	2310	2311	2312	2313	2314	2315	2316	2317	2318	2319	2320	2321	2322	2323	2324	2325	2326	2327	2328	2329	2330	2331	2332	2333	2334	2335	2336	2337	2338	2339	2340	2341	2342	2343	2344	2345	2346	2347	2348	2349	2350	2351	2352	2353	2354	2355	2356	2357	2358	2359	2360	2361	2362	2363	2364	2365	2366	2367	2368	2369	2370	2371	2372	2373	2374	2375	2376	2377	2378	2379	2380	2381	2382	2383	2384	2385	2386	2387	2388	2389	2390	2391	2392	2393	2394	2395	2396	2397	2398	2399	2400	2401	2402	2403	2404	2405	2406	2407	2408	2409	2410	2411	2412	2413	2414	2415	2416	2417	2418	2419	2420	2421	2422	2423	2424
------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------